

UNITED STATES DISTRICT COURT
 for the
 Western District of Washington

FILED	LODGED
RECEIVED	
Jun 27, 2025	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA BY _____ DEPUTY	

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 The SUBJECT DEVICES contained in the locations
 more particularly described in Attachment A.
)
)
)
)
)
)
)
 Case No. MJ25-5238

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated by reference herein.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

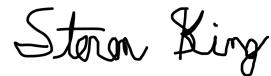
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 2111, 113(a)(6), 641, 922(o), and 26 USC 5861 and 5845	Robbery, Assault, Theft of Government Property, Unlawful Possession of a Machinegun, Unlawful Possession of Unregistered Firearms

The application is based on these facts:

See Affidavit of Special Agent Steven King

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Steven King, Special Agent

Printed name and title

This warrant is presented: by reliable electronic means telephonically recorded in person.

Date: June 27, 2025



Judge's signature

City and state: Tacoma, WA

Grady J. Leupold, United States Magistrate Judge

Printed name and title

USAO: 2025R00688

AFFIDAVIT

STATE OF WASHINGTON

) SS

COUNTY OF PIERCE

I, Steven W. King being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of any digital devices in the possession of Mario Christopher KECK, as further described in Attachment A, hereinafter the SUBJECT DEVICES. The warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Conspiracy, Robbery, Assault, and Theft of Government Property, in violation of Title 18, United States Code, Sections 371, 2111, 113(a)(6), 641, 7(3), and 2, and of the crimes of Unlawful Possession of a Machinegun and Unlawful Possession of Unregistered Firearms, in violation of Title 18, United States Code, Section 922(o) and Title 26, United States Code, Sections 5861 and 5845 have been committed by KECK and/or others known and unknown. There is also probable cause to believe that the information described in Attachment B will constitute fruits, evidence, and/or instrumentalities of these criminal violations.

2. I am a Special Agent (SA) with the Department of the Army's Criminal Investigation Division (CID), where I have been employed since April 2023. I am currently assigned to the Western Field Office (WEFO), based at Joint Base Lewis McChord, WA (JBLM), focusing on investigations involving crimes against people and

1 property, to include, but not limited to, death, sex crimes, domestic violence, assault,
 2 theft, and fraud.

3 3. As part of my duties as a Special Agent, I am authorized to conduct
 4 investigations for offenses enumerated in Title 18, United States Code, which deal with
 5 federal crimes and criminal procedure, and Title 10, United States Code, which consists
 6 of the Uniform Code of Military Justice (UCMJ), which affects the Department of the
 7 Army and the Department of Defense. My authority is derived from: (1) Title 10 U.S.C. §
 8 7377, as enacted by Congress, and (2) regulations established by the Secretary of Defense
 9 and the Secretary of the Army. As such, I am authorized to investigate violations of the
 10 law, where there is an Army interest, or which may be in the interest of the Army.

11 4. During my time with CID, I completed approximately 506 hours of
 12 instruction through the Criminal Investigator Training Program (CITP) hosted by the
 13 Federal Law Enforcement Training Center (FLETC), receiving training in areas such as
 14 physical surveillance, legal statutes, investigative procedures, financial investigations,
 15 Fourth Amendment searches, the drafting of warrant affidavits, probable cause, etc. I
 16 have also completed a 4-month field training program with CID, under the guidance of
 17 senior agents.

18 5. Previously, for approximately five years, I was employed as an investigator
 19 with the Office of the Special Commissioner of Investigation for the New York City
 20 School District (SCI), leading and participating in investigations involving criminal, civil,
 21 and administrative matters to include public corruption, property crimes, computer
 22 crimes, crimes against children, sexual misconduct, fraud, and other offenses. During my
 23 tenure with SCI, I received training and status as a New York State Peace Officer and
 24 status as a Special Patrolman with the New York City Police Department (NYPD).

25 6. The facts set forth in this Affidavit are based on my own personal
 26 knowledge; knowledge obtained from other individuals during my participation in this
 27

1 investigation, including other law enforcement officers; review of documents and records
2 related to this investigation; communications with others who have personal knowledge
3 of the events and circumstances described herein; and information gained through my
4 training and experience.

5 7. Because this Affidavit is submitted for the limited purpose of establishing
6 probable cause in support of the application for a search warrant, it does not set forth
7 each and every fact that I or others have learned during the course of this investigation. I
8 have set forth only the facts that I believe are necessary to establish probable cause of the
9 above-referenced violations.

10 8. This request is being presented electronically pursuant to Federal Rules of
11 Criminal Procedure 4.1 and 41(d)(3).

INVESTIGATION

13 9. On June 1, 2025, at about 8:05 PM, CHARLES ETHAN FIELDS and
14 LEVI AUSTIN FRAKES entered JBLM¹ through the Liberty Gate². Gate log records
15 show that FIELDS and FRAKES had their identification scanned approximately two
16 seconds apart, indicative of them being in the same vehicle while entering JBLM.
17 Surveillance footage shows a Toyota 4Runner entering JBLM through the gate when
18 FIELDS and FRAKES' identification documents were scanned. A records check
19 identified a 1997 Toyota 4Runner bearing Washington license plate CFN6396, registered
20 to FRAKES (hereinafter referred to as VEHICLE #1). Records also show FIELDS has a
21 4Runner registered in his name. Records also show that FIELDS and FRAKES reside at
22 the same residence in Lacey, WA (hereinafter referred to as RESIDENCE #1).

23 10. On June 1, 2025, at about 9:00 PM, Victim 1, a member of the United
24 States Army, entered the Charlie Company – 75th Ranger Central Operations Facility

²⁶ ¹ JBLM is a federal joint military installation housing the U.S. Army and Air Force, run by the Army, and within the special maritime and territorial jurisdiction of the United States as defined in 18 U.S.C. § 7.

²⁷ ² All persons entering JBLM are required to have their identification checked and scanned.

1 (“the Ranger compound”), located on JBLM. As Victim 1 would later explain, upon
 2 entering the facility, Victim 1 encountered two unknown persons inside. The two were
 3 partially masked and were wearing Ranger physical fitness attire. Victim 1 questioned the
 4 two persons about their presence in the compound and observed U.S. Army property
 5 clustered around them. Victim 1 directed the two persons to pull their masks down, which
 6 they did. During continued questioning from Victim 1 about the two persons’ presence in
 7 the compound, a fight ensued, at which point one of the unknown persons brandished a
 8 hammer and used it to assault Victim 1, striking Victim 1 in the head and torso, causing
 9 bodily harm and a large amount of blood loss. Victim 1 was able to fight the attackers
 10 and gain control of the hammer. Subsequently, one of the unknown persons then
 11 brandished a knife. At that point, Victim 1 surrendered. The unknown persons fled the
 12 building, with U.S. Government property, and then fled the Ranger compound.
 13 Surveillance video captured the unknown persons fleeing the area on foot while carrying
 14 rucksacks. While fleeing, the unknown persons dropped one rucksack outside the
 15 building, and then a second rucksack near the main gate of the compound. During the
 16 assault, one of the unknown persons dropped a hat, which had the name “FIELDS”
 17 handwritten on the inside.

18 11. On June 1, 2025, at about 10:00 PM, Military Police responded to the
 19 Ranger Compound, and Victim 1 was subsequently transported to Madigan Army
 20 Medical Center for evaluation of injuries.

21 12. On June 2, 2025, at about 9:00 AM, CID agents responded to Ranger
 22 compound and conducted a crime scene examination and collected a cut piece of a lock
 23 and a bolt cutter as evidence. It is likely that the two unknown persons used the bolt
 24 cutter to gain access into the facility. CID also collected disposable face masks and latex
 25 gloves from the scene. Investigators identified blood on the rucksack bag that the two
 26 persons had dropped outside the compound; some contents of the rucksack had spilled
 27

1 onto the ground and CID determined that the two unknown persons had attempted to steal
 2 approximately \$14,000.00 of U.S. Government property, most of which was recovered at
 3 the scene. That property consisted of ballistic helmets, rifle plates, and communications
 4 equipment. The ballistic plates alone are valued at approximately \$6,200.

5 13. On June 2, 2025, at about 12:00 PM, CID conducted a record check for
 6 FIELDS (the name handwritten on the inside of the hat found at the crime scene) and
 7 identified him as having entered JBLM at 8:05 PM the night before (with FRAKES).
 8 Agents also learned FIELDS had a listed residence with the Washington Department of
 9 Licensing at RESIDENCE #1. FRAKES also has a Washington driver's license with a
 10 registered address at RESIDENCE #1. A record check of personnel records maintained
 11 by the Department of Defense showed FIELDS and FRAKES residing at RESIDENCE
 12 #1. DoD records also showed FIELDS and FRAKES previously served in the military.

13 14. On June 2, 2025, at about 1:00 PM, CID conducted an interview of Victim
 14 1, who stated that had asked around his unit about the name FIELDS, based on the hat
 15 that was left at the scene. Victim 1 learned that FIELDS had been assigned to the Ranger
 16 Battalion around 2021 and was shown a photo of FIELDS by other persons in his unit.
 17 From that photo, Victim 1 identified FIELDS as one of the unknown persons who had
 18 assaulted him the night before.

19 15. On June 2, 2025, CID conducted surveillance of RESIDENCE #1. Agents
 20 observed a Black Toyota 4Runner arrive at the residence and park in the driveway, which
 21 was registered to FIELDS. During the surveillance, at about 7:24 PM, agents observed a
 22 White Toyota 4Runner, bearing Washington License Plate CRS5641 (hereinafter referred
 23 to as VEHICLE #2), arrive at RESIDENCE #1, where Agents observed two white males
 24 exit the vehicle and enter the residence. A records check identified this vehicle as being
 25 registered to Mario Christopher KECK (date of birth xx-xx-1984) at his residence in
 26 Olympia, Washington. One of the two white males was also identified as matching the
 27

1 driver's license of KECK. At about 8:00 PM, agents observed the same two white males
 2 emerge from the residence, carrying a brown and orange U-Haul cardboard box with love
 3 drab-colored fabric protruding from the top of the box, which was then placed into the
 4 White 4Runner. This material and color is consistent with several pieces of issued
 5 military equipment. Agents then observed KECK enter VEHICLE #2, while the other
 6 male entered the residence. KECK then left the area. Subsequently, agents went to the
 7 vicinity of KECK's Olympia residence. Agents noted that there was only one main road,
 8 into and out of the area where the residence was situated. At about 8:10 PM, agents
 9 observed VEHICLE #2, in the area of the residence. Agents loosely followed the vehicle,
 10 and observed that it drove towards the residence. Given that there was no other way in or
 11 out of the area and that no other vehicles matching the description of VEHICLE #2 that
 12 were observed parked in other residences, agents believed the vehicle to be parked in the
 13 residence. Further, the residence appeared to have a white SUV parked on the premises.

14 16. On June 2, 2025, CID requested and obtained a Search Warrant, issued by
 15 the Thurston County Superior Court, authorizing the search of residence of FIELDS and
 16 FRAKES, their persons, and their vehicles.

17 17. On June 2, 2025, at about 11:30 PM, CID, the Federal Bureau of
 18 Investigation (FBI), and the Thurston County Sheriff's Office (TCSO), executed the
 19 Search Warrant. While rendering the residence safe, law enforcement observed numerous
 20 firearms and explosive components. As such, CID obtained an amended Search Warrant
 21 from Thurston County Superior Court, expanding the parameters of the search. During
 22 the search, law enforcement seized numerous items of evidence, including, but not
 23 limited to, approximately 35 weapons, including rifles, pistols, short-barreled rifles, and
 24 an MG32 machine gun; weapons suppressors (i.e., silencers), some of which appear to
 25 have been 3D-printed; military property, including night vision devices, ballistic plates
 26 and plate carriers, and helmets; military munitions; and military explosives such as

1 blasting caps, flashbangs, and smoke grenades. During the search of the residence, law
 2 enforcement observed numerous Nazi/white supremacy memorabilia, murals, and
 3 literature in every bedroom and near several stockpiles of weapons and military
 4 equipment. Agents also seized personal electronic devices, clothing believed to have been
 5 worn during the assault on Victim 1, and approximately \$24,000 in cash. Agents were
 6 able to identify some of the seized items as military property due to the serial numbers
 7 and other markings on the items. I know, based on my training and experience, that some
 8 of the military items agents recovered are unlawful to possess without unique permission
 9 from the DoD and some of the items are so restricted that active-duty military members
 10 are not permitted to have or store them in their personal residences.

11 18. Agents also seized electronic devices from the residence, including devices
 12 identified as being associated with FIELDS and FRAKES.

13 19. On June 3, 2025, CID conducted an interview of FIELDS and FRAKES,
 14 both of which were advised of *Miranda* warnings; of which and one of the men agreed to
 15 speak with agents. In a recorded statement, the man acknowledged both of them
 16 (FIELDS and FRAKES) had been stealing military property from the Ranger compound
 17 for about two years, to later sell or trade. The man admitted both of them were on JBLM
 18 at the Ranger compound on June 1 to steal additional items, and a fight ensued with
 19 Victim 1. The man admitted attempts were made to burn their clothing in efforts to
 20 distance themselves from culpability.

21 20. FIELDS and FRAKES were subsequently arrested and booked into
 22 Thurston County Jail. At a hearing in Thurston County Superior Court on June 3, 2025, a
 23 judge set bail for each at \$500,000 and ordered that, if released, FIELDS and FRAKES
 24 were to be under house arrest with an ankle monitor and to have no contact with each
 25 other.

1 21. Additional investigation into FIELDS and FRAKES has shown the two
 2 have a company called “Sovereign Solutions LLC,” that advertises training and
 3 equipment. During the search of the residence, agents observed business cards associated
 4 with “Sovereign Solutions.” In the post-Miranda statement described above, one of the
 5 two men admitted that they utilized social media to trade and sell stolen property they
 6 acquired on JBLM. The man also admitted they had been selling and trading stolen items
 7 for approximately two years. Sovereign Solution’s “Formation/Registration” date is listed
 8 on the Washington Corporations and Charities Filing System website as March 14, 2023,
 9 bringing it within that approximate two-year timeframe. Sovereign Solutions’ social
 10 media accounts (on Instagram and YouTube) display items similar in appearance to the
 11 stolen military property found in FIELDS and FRAKES’ residence, but there is nothing
 12 on the publicly available social media postings about the company’s sale of the items or
 13 purchase information. However, during the post-Miranda statement referenced above,
 14 one of the men told law enforcement they used numerous social media accounts in
 15 pseudonym names to trade and sell the stolen military property. Publicly available social
 16 media content displayed weapons similar in appearance to weapons found in the
 17 residence, an individual holding a large sum of cash, and an automatic machine gun that
 18 was not found in their residence.

19 22. On June 4, 2025, FIELDS placed a call from Thurston County Jail, which
 20 was audio recorded, to his wife. The wife then put the phone on speaker, where a male,
 21 identified as Mario, was also on the call. Based on the context of the conversation and the
 22 other evidence summarized in this affidavit, I believe that the “Mario” on this call was
 23 Mario KECK. Mario told FIELDS, “You understand the meeting was today?” FIELDS
 24 asked how it went, and Mario responded that “we” needed to handle this situation,
 25 because “they are interested as fuck” and they wanted to meet next week. FIELDS told
 26 Mario he “uploaded the files to the drive” and Mario was happy to hear he had done so.
 27 Mario said he had gotten them “to the one-yard line” and they were very interested and

1 "its on." Mario identified the other apparent business owners as "Rick and Mike", and
 2 they said they just needed to "figure out the capacity." FIELDS was happy to hear this
 3 and told Mario "good job."

4 23. On June 4, 2025, the District Court for the Western District of Washington
 5 (WDWA) issued Arrest Warrants for FIELDS and FRAKES for violations of Robbery,
 6 Assault, and Theft of Government Property, based upon a Criminal Complaint.

7 24. On June 9, 2025, the District Court for the WDMA issued Search Warrants
 8 for VEHICLE #1 and digital devices seized from the residence of FIELDS and FRAKES.

9 25. On June 9, 2025, CID conducted a Digital Forensic Examination of the
 10 digital devices seized from the residence of FRAKES and FIELDS. The review of the
 11 device believed to be associated with FIELDS, identified the following:

12 a. The device had a "Journeys" where on June 1, 2025 at 9:46 PM³, the
 13 user input a GPS route from "46.973749, -122.644763", a point on Yelm Highway SE
 14 approximately 750ft south of the intersection between Yelm Highway SE and Fort Lewis
 15 Road, to "46.961998, -122.769247", a point on Dawn Hill Dr SE approximately 300ft
 16 south of the entrance to 8649 Dawn Hill Dr SE. This indicates that around the time of the
 17 events at JBLM, FIELDS likely traveled or intended to travel from JBLM to KECK's
 18 residence after the assault and theft.

19 b. A text search of "Dawn Hill Dr SE" within the devices text-based
 20 communications identified a "Mario Keck 82nd" 910-296-3122 confirming this address
 21 to be his. Further review of interactions with this contact identified Multiple calls
 22 between June 1 through June 2, 2025, and messages on June 2, 2025⁴, which read as
 23 follows:

24
 25
 26
 27 ³ The device listed the UTC. This value was converted from UTC to PST.
⁴ The device listed the UTC. This value was converted from UTC to PST.

i. 7:36 AM⁵ on June 2, 2025: "You guys good or what !!"

ii. 1:36 PM on June 2, 2025: "You good." FIELDS later responds at about 1:53 PM, stating "Yeah man all good"

c. The device contained photographs captured on May 29, 2025, which appear to have been stored in the device's gallery, depicting a firearm, what appears to be VEHICLE #2, and KECK. I believe this vehicle to be VEHICLE #2, given that the tires and front bumper in the photo stored on the phone are consistent with other observations made by agents. Additionally, the tattoos displayed in the photos stored on the phone matches social media images of KECK.



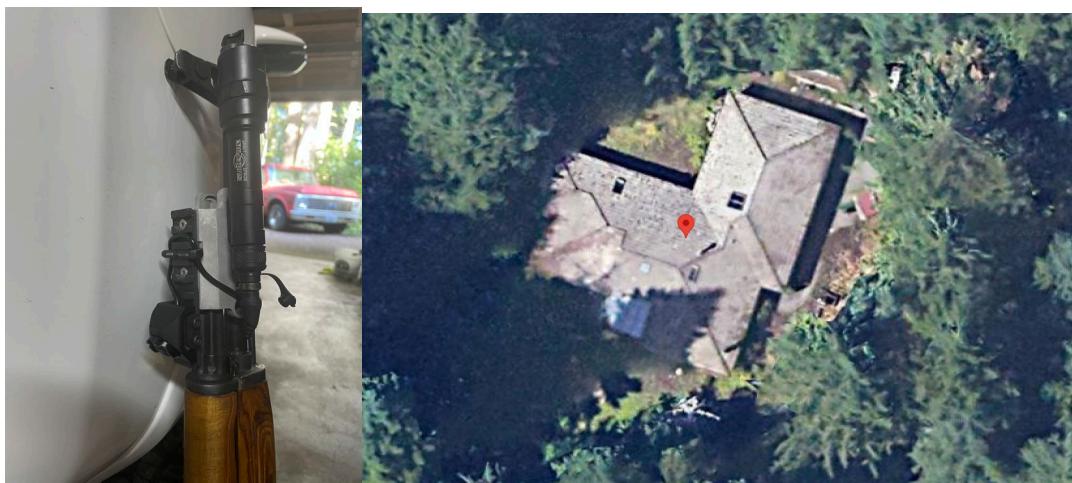
Images from the phone of FIELDS captured on May 29, 2025, believed to be of KECK and VEHICLE #2

⁵ Surveillance video shows that VEHICLE #1 returned to RESIDENCE #1 at about 7:31 AM. It's possible that KECK was contacting to FIELDS to check in, so see if FIELDS had arrived home safe from the TARGET LOCATION.



Image of KECK found on social media, displaying a rose type and snake type tattoo on the hand and arm consistent with the tattoos identified on FIELDS's phone captured on May 29, 2025.

d. Also captured by the device on May 29, 2025, and associated with the photos of KECK and VEHICLE #2, was another photo of VEHICLE #2. In the background is a wooded area and what appears to be an older model Red Ford Pickup Truck. Of note, a Google satellite image of the Target Residence shows what appears to be parked on the property, and which appears to be consistent with the image taken on May 29, 2025.



1 The image on the right was captured on FIELDS's phone on May 29, 2025. The image on the left was a
 2 satellite image from Google Maps, where the front of a red vehicle is observed, near the garage. It also
 3 appears to be parked in the same angle or manner as the photo captured on May 29, 2025.

4 e. Additional communication was identified between FIELDS and
 5 KECK, where they discuss starting a business venture together. The communications also
 6 show steps taken by FIELDS and KECK to conceal communications, where on March
 7 25, 2025, KECK mentions wanting to show FIELDS an image, and later telling FIELDS
 8 to switch to Signal⁶. The communications also show indications that KECK was aware of
 9 FIELDS's activity regarding stolen property, where on May 18, 2025, FIELDS sends a
 10 message to KECK stating "We're sitting on quite a bit just from some tacswap⁷ trades we
 11 did with a homie, but ammo is always a need. We can figure something out."

12 26. On June 11, 2025, CID interviewed FIELD's ex-girlfriend who stated that
 13 during a recent conversation with FIELDS's wife, the wife told her that prior to CID
 14 executing a Search Warrant at Residence #1, KECK had visited RESIDENCE #1 to pick
 15 up ammunition⁸.

16 27. On June 17, 2025, and June 18, 2025, CID reviewed Surveillance Video, of
 17 the area surrounding the residence of FIELDS and FRAKES:

18 a. At about 7:51 PM on June 1, 2025, VEHICLE #1 is observed
 19 leaving RESIDENCE #1.

20 b. At about 7:30 AM on June 2, 2025, VEHICLE #1 is observed
 21 returning to the residence. This is the first time VEHICLE #1 was observed returning to
 22 the RESIDENCE #1 after the events at JBLM.

23 c. During the evening of June 2, 2025, VEHICLE #2 observed by CID
 24 is seen parking across the street from RESIDENCE #1. A person who appears to be
 25 KECK is observed exiting the vehicle. Subsequently, KECK and who is believed to be

26 ⁶ Signal is an application that encrypts messages and allowing a user to mask their activity.

27 ⁷ TacSwap appears to be a website where individuals can buy, sell, or trade firearms, parts, accessories, ammunition, services, optics, or tactical kits over the internet.

28 ⁸ During the search of RESIDENCE #1, CID located and seized military ammunition and magazines.

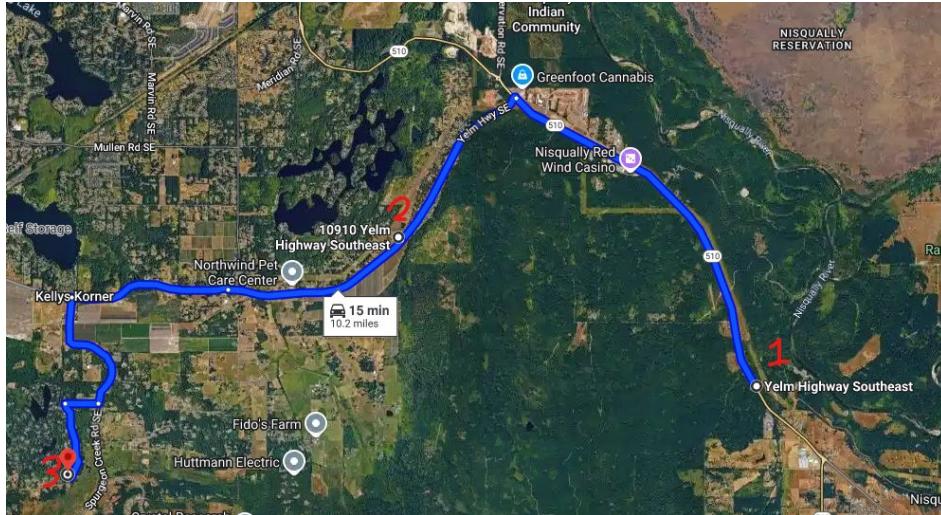
1 FIELDS, can be observed walking from Residence #1 to VEHICLE #2. KECK is
 2 observed carrying a box. While transporting the box, an item falls, which FIELDS picks
 3 up. The video contained sound, which based upon my training and experience, the item
 4 that fell appeared to be metallic in nature, and consistent with that of a metal rifle
 5 magazine (a part of a firearm), falling to the ground. This appears to be consistent with
 6 reports that KECK left the residence with ammunition.



15 VEHICLE #2 parked outside of RESIDENCE #1, with the box
 16 observed taken from RESIDENCE #1

17 d. During the evening on June 3, 2025, a person believed to be KECK
 18 is observed coming back to the house, where he talks with what is believed to be
 19 FIELDS's wife. The video also shows KECK reviewing a document, which appears to be
 20 the Search Warrant that was left at the residence.

21 28. On June 20, 2025, CID coordinated with Lacey Fire District 3, and
 22 reviewed surveillance video of Station 32 located at 10910 Yelm Highway SE, Olympia,
 23 which is along the likely path from JBLM's Ranger Compound to KECK. Agents
 24 observed that on June 1, 2025, at about 9:52 PM, a vehicle similar to that of Vehicle #1
 25 passing the fire station. The fire station is approximately 7 minutes away from the
 26 journey listed on FIELDS's phone, when he inputted a GPS route at 9:46 PM, from
 27 "46.973749, -122.644763" to "46.961998, -122.769247".



Point 1 is the from location that was inputted into the GPS of FIELDS's phone. Point 2 is the Fire Station that is believed to show VEHICLE #1 passing and Point 3 is the **Target Location**. Additionally, Surveillance Video of Residence 1, shows that VEHICLE #1 did not arrive until the morning of the June 2, 2025, the day after the incident on JBLM. As such, it's reasonable to believe that FIELDS and FRAKES traveled to KECK immediately following the incident on JBLM.

Mario Christopher KECK

29. Records maintained by the DoD, show that KECK was previously enlisted with the U.S. Army, effective 2008, and leaving active-duty service in 2014. KECK was previously convicted in Oakland, CA, in 2006 for misdemeanor possession of a concealed firearm in a vehicle.

30. Records show that KECK is associated with Killer Innovations, a company, per their mission statement "that strives every single day to engineer and produce products that change the way precision firearm parts are made and how they perform. We are always looking for the newest technology and tools to improve manufacturing processes and accuracy. If we can't find the solutions we need, we engineer and build them ourselves." The business is also associated with a Federal Firearms License for the manufacture of firearms other than destructive devices.

//

//

//

//

//

Execution of Search Warrant at KECK's Residence

31. On June 24, 2025, U.S. Magistrate Judge Grady J. Leupold issued a warrant authorizing the search of KECK's residence. The search was executed on the morning of June 25, 2025. KECK was not present because he was visiting a family member in Hayward, California. During the search, agents recovered and observed the following evidence that is pertinent to the ongoing investigation:

- Items referencing Sovereign Solutions⁹, to include stickers, design stencils, and business card;
- Correspondence addressed to FIELDS;
- Military grade magazines and ammunition to include smoke grenades and components of explosive devices, believed to be property of the U.S. Military;
- A helmet bearing a Nazi symbol consistent with symbols found in RESIDENCE #1;
- Components of a Flare System typically used on the Army's Stryker Vehicle Platform¹⁰;
- A box containing property believed to belong to the U.S. Military. This box is similar to the one agents observed KECK remove from Residence #1 and place into VEHICLE #2 following the theft from JBLM;
- A burn pit, which appeared to be fresh¹¹; and
- A stolen firearm and a short barrel shotgun.

⁹ A business of FIELDS and FRAKES which was used to sell weapon parts, consulting, and training.

¹⁰ The Stryker Vehicle is an armored vehicle, used for transporting soldiers in combat environments. JBLM has dedicated Stryker units assigned to it. The Stryker Vehicles are produced by General Dynamics, which has offices at JBLM. During the investigation, CID learned that FIELDS worked for General Dynamics for a few months, sometime after leaving the U.S. Army.

¹¹ During an interview with FIELDS, FIELDS stated that he and FRAKES burnt the clothing they wore during the robbery and assault on JBLM, which agents believe likely occurred at KECK's residence.

AFFIDAVIT OF SPECIAL AGENT KING
USAO# 2025R00688 - 15

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

1 **CELLULAR PHONES OR WIRELESS COMMUNICATION DEVICES**

2 32. Based on my training and experience, I use the following technical terms to
3 convey the following meanings:

4 a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular
5 telephone) is a handheld wireless device used for voice and data communication through
6 radio signals. These telephones send signals through networks of transmitter/receivers,
7 enabling communication with other wireless telephones or traditional “land line”
8 telephones. A wireless telephone usually contains a “call log,” which records the
9 telephone number, date, and time of calls made to and from the phone. In addition to
10 enabling voice communications, wireless telephones offer a broad range of capabilities.
11 These capabilities include: storing names and phone numbers in electronic “address
12 books;” sending, receiving, and storing text messages and e-mail; taking, sending,
13 receiving, and storing still photographs and moving video; storing and playing back audio
14 files; storing dates, appointments, and other information on personal calendars; and
15 accessing and downloading information from the Internet. Wireless telephones may also
16 include global positioning system (“GPS”) technology for determining the location of the
17 device.

18 b. Digital camera: A digital camera is a camera that records pictures as digital
19 picture files, rather than by using photographic film. Digital cameras use a variety of
20 fixed and removable storage media to store their recorded images. Images can usually be
21 retrieved by connecting the camera to a computer or by connecting the removable storage
22 medium to a separate reader. Removable storage media include various types of flash
23 memory cards or miniature hard drives. Most digital cameras also include a screen for
24 viewing the stored images. This storage media can contain any digital data, including
25 data unrelated to photographs or videos.

26 c. Portable media player: A portable media player (or “MP3 Player” or iPod)
27 is a handheld digital storage device designed primarily to store and play audio, video, or
photographic files. However, a portable media player can also store other digital data.
Some portable media players can use removable storage media. Removable storage

1 media include various types of flash memory cards or miniature hard drives. This
2 removable storage media can also store any digital data. Depending on the model, a
3 portable media player may have the ability to store very large amounts of electronic data
4 and may offer additional features such as a calendar, contact list, clock, or games.

5 d. GPS: A GPS navigation device uses the Global Positioning System to
6 display its current location. It often contains records of the locations where it has been.
7 Some GPS navigation devices can give a user driving or walking directions to another
8 location. These devices can contain records of the addresses or locations involved in such
9 navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24
10 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate
11 clock. Each satellite repeatedly transmits by radio a mathematical representation of the
12 current time, combined with a special sequence of numbers. These signals are sent by
13 radio, using specifications that are publicly available. A GPS antenna on Earth can
14 receive those signals. When a GPS antenna receives signals from at least four satellites, a
15 computer connected to that antenna can mathematically calculate the antenna's latitude,
16 longitude, and sometimes altitude with a high level of precision.

17 e. PDA: A personal digital assistant, or PDA, is a handheld electronic device
18 used for storing data (such as names, addresses, appointments or notes) and utilizing
19 computer programs. Some PDAs also function as wireless communication devices and
20 are used to access the Internet and send and receive e-mail. PDAs usually include a
21 memory card or other removable storage media for storing data and a keyboard and/or
22 touch screen for entering data. Removable storage media include various types of flash
23 memory cards or miniature hard drives. This removable storage media can store any
24 digital data. Most PDAs run computer software, giving them many of the same
25 capabilities as personal computers. For example, PDA users can work with word-
processing documents, spreadsheets, and presentations. PDAs may also include global
positioning system ("GPS") technology for determining the location of the device.

26 33. Based on my training, experience, and research, I know that cell phones
27 have capabilities that allow them to serve as a wireless telephone, digital camera, portable

1 media player, GPS navigation device, and PDA. In my training and experience,
2 examining data stored on devices of this type can uncover, among other things, evidence
3 that reveals or suggests who possessed or used the device.

4 34. Based upon my training and experience, all of these types of information
5 may be evidence of crimes under investigation. Furthermore, this application seeks
6 permission to locate not only electronically stored information that might serve as direct
7 evidence of the crimes described on the warrant, but also forensic evidence that
8 establishes how the devices were used, the purpose of its use, who used it, and when. All
9 of these types of information could constitute forensic evidence as well. Stored e-mails
10 and text messages not only may contain communications related to crimes, but also help
11 identify the participants in those crimes. Address books and contact lists may help
12 identify co-conspirators. Similarly, photographs on a cellular telephone may help identify
13 co-conspirators, either through his or her own photographs, or through photographs of
14 friends, family, and associates. Digital photographs also often have embedded location
15 data GPS information that identifies where the photo was taken. This location
16 information is helpful because, for example, it can show where co-conspirators meet,
17 where they travel, and where assets might be located. Calendar data may reveal the
18 timing and extent of criminal activity.

19 35. A cellphone used for cellular voice communication will also typically
20 contain a “call log” or “stored list of recent, received, sent or missed calls” which records
21 the telephone number, date, and time of calls made to and from the phone. The stored list
22 of recent received, missed, and sent calls is important evidence. It identifies telephones
23 recently in contact with the telephone user and may help identify co-conspirators,
24 establish a timeline of events and/or identify who was using the phone at any particular
25 time.

26 36. In addition, wireless communication devices will typically have an assigned
27 number and identifying serial number such as an ESN, MIN, IMSI, or IMEI number that
identifies the particular device on any network. This identifying information may also
include the device’s assigned name (as assigned by the user) and network addresses such

1 as assigned IP addresses and MAC addresses. I know based on my training and
2 experience that such information may be important evidence of who used a device, when
3 it was used, and for what purposes it may have been used. This information can be used
4 to obtain toll records and other subscriber records, to identify contacts by this telephone
5 with other telephones, or to identify other telephones used by the same subscriber or
6 purchased as part of a package.

7 37. Many wireless communication devices including cellular telephones such
8 as iPhones, iPads, Android phones, and other “smart phones” as well as tablet devices
9 such as Apple iPads may also be used to browse and search the Internet. These devices
10 may browse and search the Internet. These devices may browse and search the internet
11 using traditional web browsers such as Apple’s Safari browser or Google’s Chrome
12 browser as well as through third-party applications such as Facebook, Twitter and other
13 that also provide the ability to browse and search the Internet. Based on my training and
14 experience, I know that Internet browsing history may include valuable evidence
15 regarding the identity of the user of the device. This evidence may include online user
16 names, account numbers, e-mail accounts, and bank accounts as well as other online
17 services. Internet browsing history may also reveal important evidence about a person’s
18 location and search history. Search history is often valuable evidence that may help
19 reveal a suspect’s intent and plans to commit a crime or efforts to hide evidence of a
20 crime and may also help reveal the identity of the person using the device.

21 38. Cellphones and other wireless communication devices are also capable of
22 operating a wide variety of communication application or “Apps” that allow a user to
23 communicate with other devices via a variety of communication channels. These
24 additional communication channels include traditional cellular networks, voice over
25 Internet protocol, video conferencing (such as FaceTime and Skype), and wide variety of
26 messaging applications (such as SnapChat, What’sApp, Signal, Telegram, Viber and
27 iMessage). I know based on my training and experience that there are hundreds of
different messaging and conferencing applications available for popular cellular
telephones and that the capabilities of these applications vary widely for each application.

1 Some applications include end-to-end encryption that may prevent law enforcement from
2 deciphering the communications without access to the device and the ability to “unlock”
3 the device through discovery of the user’s password or other authentication key.

4 39. Other communication applications transmit communications unencrypted
5 over centralized servers maintained by the service provider and these communications
6 may be obtained from the service provider using appropriate legal process. Other
7 applications facilitate multiple forms of communication including text, voice, and video
8 conferencing. Information from these communication apps may constitute evidence of
9 crimes under investigation to the extent they may reveal communications related to the
10 crime or evidence of who the user of the device was communicating with and when those
11 communications occurred. Information from these communication apps may also reveal
12 alias names used by the device owner that may also lead to the other evidence.

13 40. I know based on my training and experience that obtaining a list of all the
14 applications present on a cellphone may provide valuable leads in an investigation. By
15 determining what applications are present on a device, an investigator may conduct
16 follow-up investigation including obtaining subscriber records and logs to determine
17 whether the device owner or operator has used each messaging application. This
18 information may be used to support additional search warrants or other legal process to
19 capture those communications and discover valuable evidence.

20 41. Cellphones and other wireless communication devices may also contain
21 geolocation information where the device was at particular times. Many of these devices
22 track and store GPS and cell-site location data to provide enhanced location-based
23 services, serve location-targeted advertising, search results, and other content. Numerous
24 applications available for wireless communication devices collect and store location data.
25 For example, when location services are enabled on a handheld mobile device, many
26 photo applications will embed location data with each photograph taken and stored on the
27 device. Mapping applications such as Google Maps may store location data including
lists of locations the user has entered into the application. Location information may
constitute evidence of the crimes under investigation because that information may reveal

1 whether a suspect was at or near the scene of a crime at any given moment and may also
2 reveal evidence related to the identity of the user of the device.

3 42. Based on my training and experience, and research, I know that cellular
4 phone devices have capabilities that allow them to function as wireless telephones, digital
5 camera, portable media player, GPS navigation device, and "PDA." In my training and
6 experience, examining data stored on devices of this type can uncover, among other
7 things, evidence that reveals or suggests who possessed or used the device. In my training
8 and experience, smart phones can act as minicomputers in that they have many of the
functionalities of traditional computers.

9 43. The warrant I am applying for would permit law enforcement to obtain
10 from certain individuals the display of physical biometric characteristics (such as
11 fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to
12 search and seizure pursuant to this warrant. I seek this authority based on the following:

13 a. I know from my training and experience, as well as from
14 information found in publicly available materials published by device manufacturers, that
15 many electronic devices, particularly newer mobile devices, offer their users the ability to
16 unlock the device through biometric features in lieu of a numeric or alphanumeric
17 passcode or password. These biometric features include fingerprint scanners and facial
18 recognition features. Some devices offer a combination of these biometric features, and
the user of such devices can select which features they would like to utilize.

19 b. If a device is equipped with a fingerprint scanner, a user may enable
20 the ability to unlock the device through his or her fingerprints. For example, Apple offers
21 a feature called "Touch ID," which allows a user to register up to five fingerprints that
22 can unlock a device. Once a fingerprint is registered, a user can unlock the device by
23 pressing the relevant finger to the device's Touch ID sensor, which is found in the round
24 button (often referred to as the "home" button) located at the bottom center of the front of
25 the device. The fingerprint sensors found on devices produced by other manufacturers
26 have different names but operate similarly to Touch ID.

1 c. If a device is equipped with a facial recognition feature, a user may
2 enable the ability to unlock the device through his or her face. For example, Apple offers
3 a facial recognition feature called “Face ID.” During the Face ID registration process, the
4 user holds the device in front of his or her face. The device’s camera then analyzes and
5 records data based on the user’s facial characteristics. The device can then be unlocked if
6 the camera detects a face with characteristics that match those of the registered face.
7 Facial recognition features found on devices produced by other manufacturers have
8 different names but operate similarly to Face ID.

9 d. In my training and experience, users of electronic devices often
10 enable the aforementioned biometric features because they are considered to be a more
11 convenient way to unlock a device than by entering a numeric or alphanumeric passcode
12 or password. Moreover, in some instances, biometric features are considered to be a more
13 secure way to protect a device’s contents. This is particularly true when the users of a
14 device are engaged in criminal activities and thus have a heightened concern about
securing the contents of a device.

15 e. As discussed in this affidavit, based on my training and experience I
16 believe that one or more digital devices will be found during the search. The passcode or
17 password that would unlock the device(s) subject to search under this warrant is not
18 known to law enforcement. Thus, law enforcement personnel may not otherwise be able
19 to access the data contained within the device(s), making the use of biometric features
necessary to the execution of the search authorized by this warrant.

20 f. I also know from my training and experience, as well as from
21 information found in publicly available materials including those published by device
22 manufacturers, that biometric features will not unlock a device in some circumstances
23 even if such features are enabled. This can occur when a device has been restarted,
24 inactive, or has not been unlocked for a certain period of time. For example, Apple
25 devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed
26 since the device was last unlocked or (2) when the device has not been unlocked using a
27 fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156

1 hours. Biometric features from other brands carry similar restrictions. Thus, in the event
 2 law enforcement personnel encounter a locked device equipped with biometric features,
 3 the opportunity to unlock the device through a biometric feature may exist for only a
 4 short time.

5 44. Due to the foregoing, I request that during the execution of the search of
 6 any Apple brand device(s) (such as an iPhone or iPad) or Android Device(s) which law
 7 enforcement with reasonable particularity believe are in the possession or control of
 8 KECK, for the purpose of attempting to unlock the device(s) via biometric authentication
 9 in order to search its contents as authorized by this warrant, law enforcement personnel
 10 be authorized: (i) to press the fingers, including thumbs, of Mario KECK to sensors of the
 11 device, using no more than reasonable force, or (ii) to hold up the device in front of the
 12 face of KECK.

12 SEARCH TECHNIQUES

13 45. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 14 Rules of Criminal Procedure, the warrant I am applying for will permit imaging or
 15 otherwise copying all data contained on the subject devices and will specifically
 16 authorize a review of the media or information consistent with the warrant.

17 46. In accordance with the information in this affidavit, law enforcement
 18 personnel will execute the search of the subject pursuant to this warrant as follows:

19 a. **Securing the Data**

20 47. i. In order to examine the ESI in a forensically sound manner, law
 21 enforcement personnel with appropriate expertise will attempt to produce a complete
 22 forensic image, if possible and appropriate, of the subject devices.

23 48. ii. Law enforcement will only create an image of data physically
 24 present on or within the subject devices. Creating an image of the subject devices will not
 25 result in access to any data physically located elsewhere. However, a subject devices that
 26 have previously connected to devices at other locations may contain data from those
 27 other locations.

b. Searching the Forensic Images

2 49. Searching the forensic images for the items described in Attachment B may
3 require a range of data analysis techniques. In some cases, it is possible for agents and
4 analysts to conduct carefully targeted searches that can locate evidence without requiring
5 a time-consuming manual search through unrelated materials that may be commingled
6 with criminal evidence. In other cases, however, such techniques may not yield the
7 evidence described in the warrant, and law enforcement may need to conduct more
8 extensive searches to locate evidence that falls within the scope of the warrant. The
9 search techniques that will be used will be only those methodologies, techniques and
10 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the
items authorized to be seized pursuant to Attachment B to this affidavit.

11 50. Searching a cellular phone or wireless communication device is frequently
12 different than conducting a search of a traditional computer. Agents and forensic
13 examiners will attempt to extract the contents of the cellular phone or wireless
14 communication device using a variety of techniques designed to accurately capture the
15 data in a forensically sound manner in order to make data available to search of items
16 authorized by the search warrant. This may involve extracting a bit-for-bit copy of the
17 contents of the device or, if such an extraction is not feasible for any particular device,
18 the search may involve other methods of extracting data from the device, such as copying
19 the device's active user files (known as a logical acquisition) or copying the device's
20 entire file system (known as a file system acquisition). If none of these methods are
21 supported by the combination of tools available to the examiner and the device to be
22 searched, the agents and examiners may conduct a manual search of the device by
23 scrolling through the contents of the device and photographing the results. Based on the
24 foregoing and consistent with Rule 41(e)(2)(B), the warrant I am applying for would
25 permit seizing, imaging, or otherwise copying the subject devices and would authorize a
26 later review of the media or information consistent with the warrant. The later review

1 may require techniques, including but not limited to computer-assisted scans of the entire
 2 medium, that might expose many parts of a hard drive to human inspection in order to
 3 determine whether it is evidence described by the warrant.

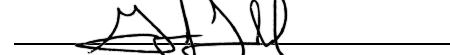
4 **CONCLUSION**

5 51. Based on the foregoing, I submit there is probable cause to believe that
 6 contained within the locations described in Attachment A, there exists evidence, fruits,
 7 and instrumentalities, as described in Attachment B, of violations of Conspiracy,
 8 Robbery, Assault, and Theft of Government Property, in violation of Title 18, United
 9 States Code, Sections 371, 2111, 113(a)(6), 641, 7(3), and 2, and of the crimes of
 10 Unlawful Possession of a Machinegun and Unlawful Possession of Unregistered
 11 Firearms, in violation of Title 18, United States Code, Section 922(o) and Title 26,
 12 United States Code, Sections 5861 and 5845.

13 
 14

15 STEVEN W. KING, Affiant
 16 Special Agent
 17 U.S. Army Criminal Investigation
 18 Division

19 The above-named agent provided a sworn statement to the truth of the foregoing
 20 affidavit by telephone on the 27th day of June 2025.

21 
 22 GRADY J. LEUPOLD
 23 United States Magistrate Judge

ATTACHMENT A

The property to be searched is:

(a) the person of Mario Christopher KECK, date of birth xx-xx-1984, including any briefcase, backpack, or other bag in his possession; and

(b) a white Toyota 4Runner bearing Washington License Plate CRS5641;

to recover any cellular devices, including smartphones and tablets.

ATTACHMENT B

Things to be Searched for and Seized

From the locations described in Attachment A, the government is authorized to search any cellular device, such as a smartphone or tablet, for evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 371, 2111, 113(a)(6), 641, 7(3), and 2, and Title 18, United States Code, Section 922(o) and Title 26, United States Code, Sections 5861 and 5845, committed CHARLES ETHAN FIELDS, LEVI AUSTIN FRAKES, and MARIO CHRISTOPHER KECK, on or about June 1, 2025, including the following:

- a. Assigned phone number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored photographs, videos, addresses, calendar notes, notes, map history, or documents/files of or related to the crimes under investigation, and/or the user of the phone or suspected co-conspirators, including any embedded GPS data or other metadata associated with those photographs, videos, and other items;
- e. Stored text messages related to the aforementioned crimes of investigation, including iMessages, WhatsApp messages, or other similar messaging services where the data is stored on the telephone;
- f. Stored emails related to the aforementioned crimes of investigation;
- g. Stored voicemails related to the aforementioned crimes of investigation;
- h. Stored web browsing history related to the aforementioned crimes of investigation;

- 1 i. Stored social media content/history related to the aforementioned crimes
- 2 of investigation;
- 3 j. Stored banking or money transfer history, including application-based
- 4 money transfer data/history (e.g., CashApp account data/history); and
- 5 k. Stored location data, including from any map applications on the phone.

6 During the execution of the search of any Apple brand device(s) (such as an
7 iPhone or iPad) or Android Device(s) which law enforcement with reasonable
8 particularity believe are in the possession or control of MARIO KECK: For the purpose
9 of attempting to unlock the device(s) via biometric authentication in order to search its
10 contents as authorized by this warrant, law enforcement personnel are authorized: (i) to
11 press the fingers, including thumbs, of KECK to sensors of the device(s), using no more
12 than reasonable force, or (ii) to hold up the device(s) in front of the face of KECK.